deviceTRUST

Contextualizing IT

Simple. Dynamic. Integrated.

Use Case Übersicht

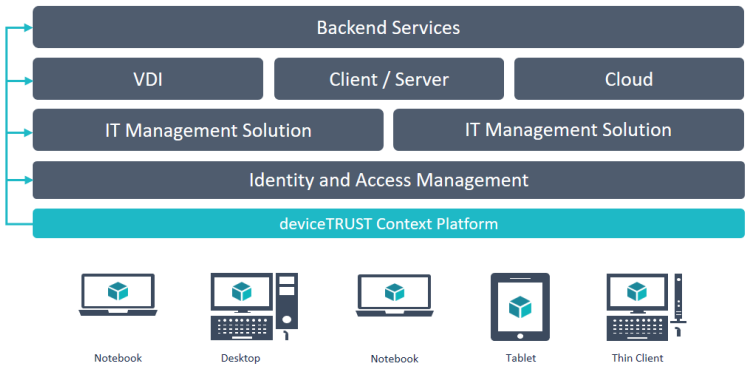
deviceTRUST bietet die zentrale Kontextplattform für Unternehmen, die es Anwendern ermöglicht von jedem Ort, mit jedem beliebigen Endgerät, über jedes Netzwerk und zu jeder Zeit mit ihrem digitalen Workspace zu Arbeiten und gibt den IT-Abteilungen gleichzeitig die erforderlichen Informationen und Kontrolle zur Einhaltung aller Sicherheits-, Compliance- und regulatorischer Vorgaben.

Mit seinen zum Patent angemeldeten Technologien stellt deviceTRUST mehr als 200 Hardware-, Software-, Netzwerk-, Sicherheits-, Performance- und Standorteigenschaften bereit. deviceTRUST lässt sich problemlos in jede bestehende Workspace-Management-Lösung integrieren und benötigt keine zusätzliche Infrastruktur. Der Kontext ist immer aktuell und jede Änderung löst eine definierbare Aktion aus.

deviceTRUST - Contextualizing IT

Einsatzszenarien

- Kontrolle von Device-basierten Lizenzen
- Standortbezogener Zugriff auf Netzwerkdrucker und Laufwerke
- Zugriff externer Mitarbeiter
- Zugriffssteuerung aus Wi-Fi Netzen
- Einhaltung der Compliance Vorgaben in Bezug auf die Endgerätesicherheit
- Steuerung des Zugriffs auf eine Sicherheitsrelevante Anwendung (double-hop)



deviceTRUST

Telefon: +49 (6162) 8015950
E-Mail: info@devicetrust.com
Internet: https://devicetrust.com
Twitter: @deviceTRUST

deviceTRUST

Contextualizing IT

Simple. Dynamic. Integrated.

Use Case Übersicht

Kontrolle von Device-basierten Lizenzen

Die bei einem Kunden eingesetzten Anwendungen sind Aufgrund der Lizenzbedingungen des Herstellers pro Endgerät zu lizenzieren. Diese Anwendungen werden jedoch über die Terminal Serverplattform mit Citrix XenApp den Mitarbeitern bereitgestellt. Hieraus ergibt sich die Problematik, dass die Anwendungen von jedem Mitarbeiter und jedem Endgerät genutzt werden können. Um die Bereitstellung dieser Anwendungen lizenzkonform umzusetzen, war es zwingend erforderlich das verbundene Endgerät eindeutig zu identifizieren. deviceTRUST liefert die benötigten Information über die Seriennummer des verbundenen Endgerätes in die virtuelle Sitzung. Diese Informationen in Verbindung mit der bei dem Kunden eingesetzten Management Lösung ermöglichen es den Zugriff auf die entsprechenden Anwendungen zuzulassen bzw. zu unterbinden. Somit ist eine Bereitstellung entsprechend den Lizenzbedingungen des Herstellers sichergestellt.

Sicherheit	●○○
Compliance	●●●
Konfiguration	●●○

Standortbezogener Zugriff auf Netzwerkdrucker und Laufwerke

In einem international agierenden Unternehmen mit verschiedenen Standorten sowie Mitarbeitern die zwischen den einzelnen Standorten pendeln, wird der Zugriff auf die Unternehmensanwendungen mittels einer VDI Plattform ermöglicht. Herbei ist es erforderlich, dass die Mitarbeiter basierend auf dem jeweiligen Standort im Unternehmen Zugriff auf die entsprechenden lokalen Ressourcen wie Netzwerkdrucker und Netzlaufwerke erhalten. deviceTRUST stellt innerhalb der virtuellen Sitzung detaillierte Informationen über den aktuellen Standort des verbundenen Endgerätes zur Verfügung und ermöglicht eine entsprechende Zuordnung der Ressourcen mittels Microsoft GPO-Skripte und GPP-Aktionen.

Sicherheit	●○○
Compliance	●●○
Konfiguration	●●●

Zugriff externer Mitarbeiter

Mitarbeiter eines externen Lieferanten benötigen Zugriff auf die zentral auf Terminal Servern bereitgestellten Unternehmens-anwendungen. Neben der Benutzerauthentifizierung ist es aus Sicherheitsgründen erforderlich, dass die externen Mitarbeiter ausschließlich von ihren firmeneigenen Endgeräten auf die zentrale Plattform zugreifen. deviceTRUST wird hier genutzt, um bei der Anmeldung sowie während der gesamten Laufzeit der virtuellen Sitzung sicherzustellen, dass das verbundene Endgerät zum einen Mitglied der jeweiligen Domäne des Lieferanten ist und darüber hinaus der Mitarbeiter auf diesem Endgerät über keine administrativen Rechte verfügt. Das Unternehmen stellt somit sicher, dass Zugriffe der Lieferanten ausschließlich entsprechend den internen Vorgaben erfolgen.

Sicherheit	●●●
Compliance	●●●
Konfiguration	●○○

Zugriffssteuerung aus WI-FI Netzen

Das Unternehmen möchte seinen Mitarbeitern die Möglichkeit geben zu jeder Zeit und von jedem Ort auf die mittels Terminal Servern bereitgestellten Unternehmensanwendungen und Ressourcen zugreifen zu können. Hierzu zählen auch Anwendungen mit sensiblen Daten. Eine Steuerung der Zugriffe lediglich auf Basis der Gruppenmitgliedschaft des Benutzers reichte in diesem Fall nicht aus. Das Unternehmen muss sicherstellen, dass ein Mitarbeiter der sich mit seinem verbundenen Endgerät in einem unverschlüsselten WI-FI Netzwerk befindet zwar grundsätzlich Zugriff auf die zentrale Plattform hat, jedoch Anwendungen mit sensiblen Daten, in diesem Fall die Personaldaten, nicht verfügbar sind. Hiermit soll verhindert werden, dass der Mitarbeiter in einem öffentlichen Bereich kritische Personaldaten auf seinem Bildschirm anzeigen kann. deviceTRUST stellt die Information über das verbundene WI-FI Netzwerk und dessen Verschlüsselung durchgängig aktuell zur Verfügung.

deviceTRUST

Contextualizing IT

Simple. Dynamic. Integrated.

Use Case Übersicht

Hierdurch ist es für das Unternehmen möglich mit den vorhandenen Managementlösungen den Zugriff auf die sensiblen Anwendungen entsprechend den Vorgaben umzusetzen.

Sicherheit	●●●
Compliance	●○○
Konfiguration	●○○

Einhaltung der Compliance Vorgaben in Bezug auf die Endgerätesicherheit

Ein Unternehmen ermöglicht den Mitarbeitern sowohl von unternehmenseigenen als auch von privaten Endgeräten auf die VDI Umgebung zuzugreifen. Die internen Vorgaben legen fest, dass ein verbundenes Endgerät während der gesamten Laufzeit der virtuellen Sitzung über eine aktive Firewall sowie einen aktiven Virenscanner verfügen muss. Sollte eine der Sicherheits-komponenten nicht aktiv oder nicht auf dem aktuellen Stand sein muss die Benutzersitzung umgehend getrennt werden. Mittels deviceTRUST wird sichergestellt, dass der Status der Firewall sowie des Virenscanners während der gesamten Laufzeit immer aktuell in der virtuellen Sitzung verfügbar ist. Die dynamischen Trigger von deviceTRUST stellen zudem sicher, dass jede Veränderung der Sicherheitskomponenten unverzüglich zu einer gesteuerten Aktion führt und die Sitzung des Mitarbeiters getrennt wird. Hierdurch wurden die internen Vorgaben der IT-Sicherheitsabteilung umgesetzt und den Mitarbeitern eine flexible und sichere Arbeitsumgebung zur Verfügung gestellt.

Sicherheit	●●○
Compliance	●●●
Konfiguration	●○○

Steuerung des Zugriffs auf eine sicherheitsrelevante Anwendung (double-hop)

Ein Unternehmen stellt die gesamte Arbeitsplatzumgebung mittels einer VDI Umgebung zur Verfügung. Einige Anwendungen werden dann von einer Terminal Serverfarm als veröffentlichte Anwendung in der VDI Umgebung bereitgestellt (double-hop). Die Anforderung des Unternehmens ist es, dass eine kritische Anwendung mit personenbezogenen Daten ausschließlich ausgeführt werden darf, wenn sich sowohl das verbundene Endgerät als auch der Benutzer in einem definierten Bereich (Netzwerksegment) des Unternehmens befinden. Sollte das Endgerät den Bereich verlassen oder die Sitzung von einem anderen Endgerät außerhalb dieses Bereiches übernommen werden, muss sichergestellt sein, dass die kritische Anwendung umgehend beendet wird. Zusätzlich ist es erforderlich, dass der Benutzer sich tatsächlich an dem verbundenen Endgerät befindet und dieses nicht Remote gesteuert wird. deviceTRUST stellt in dieser Umgebung sicher, dass innerhalb der virtuellen Sitzung jederzeit die Information über das genutzte Netzwerk und die Nutzung des Endgerätes (Ist das Endgerät remotegesteuert?) aktuell zur Verfügung stehen. Die integrierten deviceTRUST Trigger werden genutzt um eine in dem Unternehmen bereits eingesetzte Softwarelösung zu triggern welche die kritische Anwendung beendet. Das Unternehmen kann somit seine Sicherheits-anforderungen einhalten und einen produktiven Betrieb sicherstellen.

Sicherheit	●●○
Compliance	●●●
Konfiguration	●○○